VULNERABILITY OF WIRELINE AND CELLULAR TELECOMMUNICATIONS NETWORKS TO HIGH POWER RADIO FREQUENCY FIELDS

Perry Wilson[1], Eldon Haakinson[2], Roger Dalke[2]

High level electromagnetic fields can upset and damage electronics, as well as disrupt or disable computer software. Thus, high power radio frequency (RF) fields pose a threat to critical infrastructures such as telecommunications. This report examines the vulnerability of public and emergency telecommunications networks to high power RF fields, at the network and nodal levels. The assessment of network level vulnerability requires an examination of the system architecture and how redundancy and robustness are used to compensate for nodal loss or overload. The overall public telecommunications network has sufficient redundancy and capacity to withstand the loss of even multiple nodes. A full system collapse is not envisioned as a possible scenario. However, large local blackouts are possible. The assessment of nodal level vulnerability involves estimating the coupling of high level RF fields to sensitive equipment located at a node. Neither public network switching stations nor cellular base stations are intentionally hardened against high level RF fields. Typical steel reinforced concrete walls provide little shielding for frequencies above a few hundred MHz. Thus, a switching station could be disrupted (10 to 100 thousand users) by a high power RF device in this frequency range, although the probability of disruption is difficult to assess due to the variety and complexity of building layouts. Wireless base stations are highly vulnerable to high power fields coupling via the antennas.

Key words: critical infrastructure protection, high power RF fields, public switched telephone network, shielding, vulnerability

1. INTRODUCTION

High level electromagnetic fields can upset and damage electronics, as well as disrupt or disable computer software (e.g., [1]). Thus, high power radio frequency (RF) fields pose a threat to electronics and software dependent systems. In particular, critical infrastructures such as public and private telecommunications networks could be affected. The objective of this study is to briefly assess whether high power RF fields could significantly disrupt public and emergency telecommunications systems.

[1] The author is with the National Institute of Standards and Technology, U.S. Department of Commerce, Boulder, CO 80305. The author was with the Institute for Telecommunication Sciences when the work was done.

[2] The authors are with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO 80305.

A telecommunications network may be viewed as a set of nodes (e.g., collection and routing points) connected by links (e.g., wires, fibers, wireless radio paths). The following questions will be addressed.

- Can the loss of a node (or nodes) cascade through the telecommunications network causing a large-scale system blackout or crash?

- Can high power fields disrupt or disable a node (such as a switching station or a wireless base station)?

The first question addresses network vulnerability and requires an examination of how redundancy and robustness within a network are used to compensate for nodal loss or overload. This report will primarily address the public switched telephone network. Other networks such as cellular networks or the Internet are either interfaced to, or piggybacked on the switched network. Emergency networks are usually stand-alone and will be only briefly discussed. The second question addresses nodal vulnerability and involves estimating the coupling of high level RF fields to sensitive equipment located at a nodal location. In particular, switching stations (i.e., buildings that house switching equipment) and cellular base stations (i.e., antenna towers and associated equipment sheds) are considered.

The high power RF devices assumed here are characterized by powers in the MW to GW range at frequencies between approximately 800 MHz and 30 GHz. The 800 MHz practical lower limit is due primarily to two factors. First, high gain antennas become too large for easy concealment and mobility much below 1 GHz. Second, RF power becomes significantly more expensive at lower frequencies.

It needs to be emphasized that the results presented in this report are preliminary. The telecommunication network architectures are considered at a very general level only. The penetration of RF fields into buildings is simplified to a two-dimensional model in order to show basic trends. The coupling to a more realistic three-dimensional model is not considered. The complex problem of field coupling to a complex layout of equipment and interconnections is also not considered. Nonetheless, some initial conclusions may be drawn as to the potential vulnerability of wireline and cellular telecommunication networks. We hope that this report will serve as a basis for more detailed future studies.

The report is organized as follows. Section 2 reviews basic telecommunications networks and their system architectures. Nodal types within the system are identified, their functions briefly described, and the impact of their loss evaluated. Section 3 examines the physical location of system nodes and assesses their vulnerability to high power RF fields. Section 4 summarizes results. Appendices A and B give details as to the calculation of field penetration through reinforced concrete and shielded cables.

2. NETWORK LEVEL VULNERABILITY

Telecommunications, broadly defined, includes all forms of electronic voice and data communications systems: public, private, emergency, government, and military; wire, fiber, and wireless; overhead and buried; ground-based and satellite. Telecommunications systems considered here are:

- Public Switched Telephone Network
- Internet
- Cellular
- Private Radio Networks (Specialized Mobile Radio, Public Safety, Law Enforcement)

The Public Switched Telephone Network (PSTN) is the oldest telecommunications network to span the U.S. and is still in existence today. Once the call is set up, the circuit remains "connected" between the caller and called party until one of them hangs up. The system architecture has evolved to make it very robust and able to handle varying loads and system outages.

The Internet spans the U.S. using much of the PSTN as its backbone along with its own partial network. The Internet sends all data from source to destination by breaking the original message into packets with each packet containing the addresses of the destination as well as the source. It uses a connectionless scheme to transmit the information allowing each packet to find its own route through the network.

Cellular Mobile Telephone Service and Personal Communication Service (PCS) systems use wireless means to link mobile subscribers to each other, to the PSTN, or to the Internet. Once a call is set up, the subscriber can move from cell to cell within the network while maintaining access.

Private Radio Network (e.g., Specialized Mobile Radio, Public Safety, Transportation, Public Utility) systems provide mobile users access to other mobile users of the same network or to local area networks (LANs) on the network. These are typically stand-alone networks. Thus, they do not always tie the mobile user to the PSTN or the Internet, although such a link is possible. The systems can be small to serve a community, or large to serve a city or a state, or can span the U.S. to serve a particular industry.

This report will mainly focus on the PSTN and cellular systems, since these affect the largest set of users. The Internet, which piggybacks the PSTN network, and private and emergency networks will be only briefly discussed.

2.1 Telecommunication System Architectures

Telecommunication systems have traditionally been either stand-alone wireline or stand-alone wireless systems. The typical stand-alone wireline system is a switched telephone

circuit that connects one telephone user with another. The typical stand-alone wireless telecommunication system allows mobile radio users to communicate with each other or with a base station radio and dispatcher. The stand-alone wireline system is independent of the wireless system (although it might have microwave relay (wireless) links to connect portions of the network). Conversely, the stand-alone wireless system is independent of the wireline system and its features.

From these traditional concepts, the separate wireless and wireline systems have evolved into systems that require both wireline and wireless components and networks in order to provide the features that users demand. The seamless integration of the networks also provides connectivity to other users who are not normally accessible on either the wireline or wireless networks.

This high level of interconnectivity means that breaks in one system (e.g. wireless), due to a software failure for example, could propagate into another system (e.g. wireline). Interconnectivity, however, also leads to robustness by providing alternate links to compensate for any single lost link. Indeed, rapidly expanding interconnectivity and capacity is likely to decrease the vulnerability of the overall telecommunications network to the failure of any particular subset of the system.

2.1.1 Public Switched Telephone Network

During the late 1940s and early 1950s, the PSTN underwent an architectural evolution in order to offer direct distance dialing (DDD). The network was structured to be hierarchical so that a call originating at one end office (alternately termed a local or central office) would be routed up, across, and down the structure to the destination end office. Figure 1 shows the concept of tiers consisting of switching centers for routing telephone calls. Business and residential phones are connected by wireline to an end office switch. If the calling and called telephones are connected to the same switch, the call is routed directly within the switch. If the called telephone is not connected to the switch, the call needs to be routed up in the tier to the switch that is common to both the calling and called telephones. Figure 2 shows the 5-tier hierarchical structure used for many years by the Bell System and uses the nomenclature of the Bell System to identify the switching centers in the hierarchy.

Up to 10,000 lines could be connected to one end office switch handling the prefix NNN to give the numbering sequence NNN-XXXX. Additional prefixes (NNA, NNB etc.) can be handled within a single end office. Thus an end office can have anywhere from 10,000 to 100,000 subscriber lines. At this point, there is normally no redundancy built into the system from the residence or business to the end office switch. That is, if the end office switch is unable to handle the call due to either heavy use or a physical disruption, then the telephone user will be without service until the load eases or the physical problem is repaired.

The above simple hierarchical system is now replaced by a dynamic routing system. This dynamic system consists of two basic parts; the switching system and the signaling system.

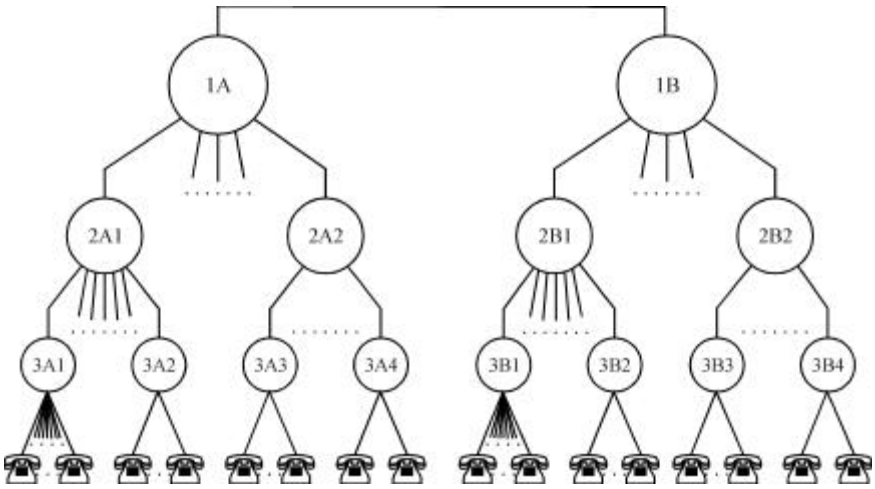

Figure 1. Tiered switching centers.

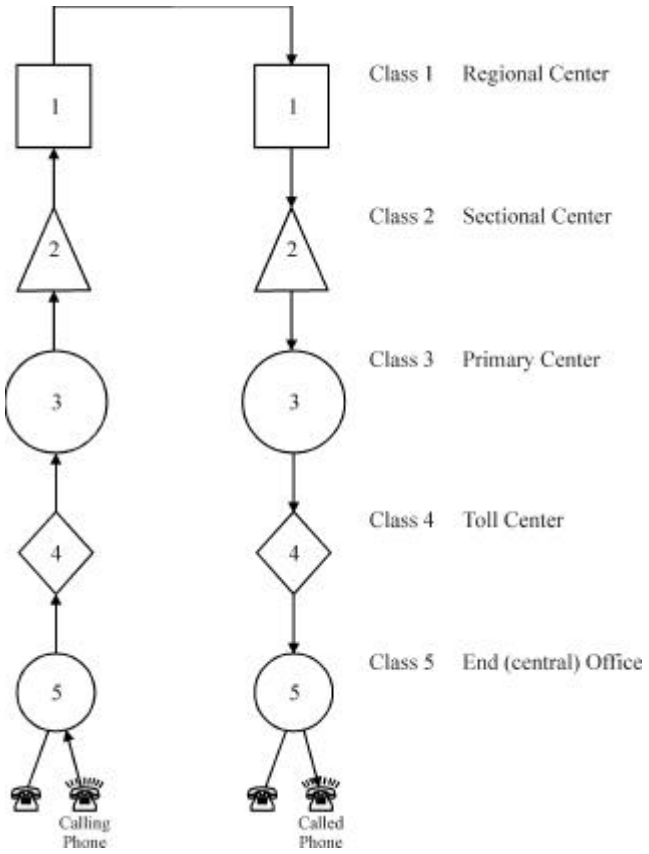

Figure 2. Bell system 5-tier hierarchical structure.

The switching system (hardware) creates the physical wireline connection between users. The signaling system (software) checks for the availability of connections and routes, monitors traffic, controls system logic, and collects billing data. Breaks in these two systems will affect the overall system differently. These two systems, switching and signaling, are discussed in more detail in the next two sections.

2.1.1.1 Switching System

The switching system creates the physical wireline connection between users. If the call's destination is at another end office, then the call is routed up the hierarchy until the appropriate crossover point is reached for routing the call to the destination end office. The structure ties several end offices to a toll center, several toll centers to a primary center, etc. Finally, the call might reach the regional center for routing to another regional center. For example, there were 10 regional centers in this hierarchy within the U.S. and the centers represented the last possible route for the telephone call.

Although this hierarchy works for completing calls, it forces each call through many intermediate-switching centers that could be avoided if additional trunks are made available. These trunks (called High Usage circuits) were added between switching centers where usage statistics showed they were economically valuable. Figure 3 shows routes in place between switching centers available for high usage links. The switches are programmed to route calls along the various route choices depending upon loading at the individual switches. Routing algorithms attempt to limit the number of switching centers that the call must go through.

In the mid 1980s, the Bell System began using fourth generation Electronic Switching System (ESS) switches which allow high-speed dialing throughout the network and use computer-controlled intelligence to select the best routes for the calls. The system uses Dynamic Nonhierarchical Routing (DNHR) which eliminates the 5-tier hierarchy and allows pre-planned routes between switches to change dynamically throughout the day. Figure 4 shows the structure of DNHR with first choice routes for call setup but also many alternate routes as well. The objective is to maximize the use of the existing network to route calls efficiently and quickly without adding more switches and switch centers to the existing network. The result also provides reliability to the network: if a switch center is overloaded, telephone traffic can be routed around the busy switch. But equally important, if a switch center has suffered a loss of capacity or capability due to a natural disaster or equipment failure, the network will be virtually unaffected except for some loss of redundancy and capacity. Calls will be routed around the impaired switch center until the problem is corrected.

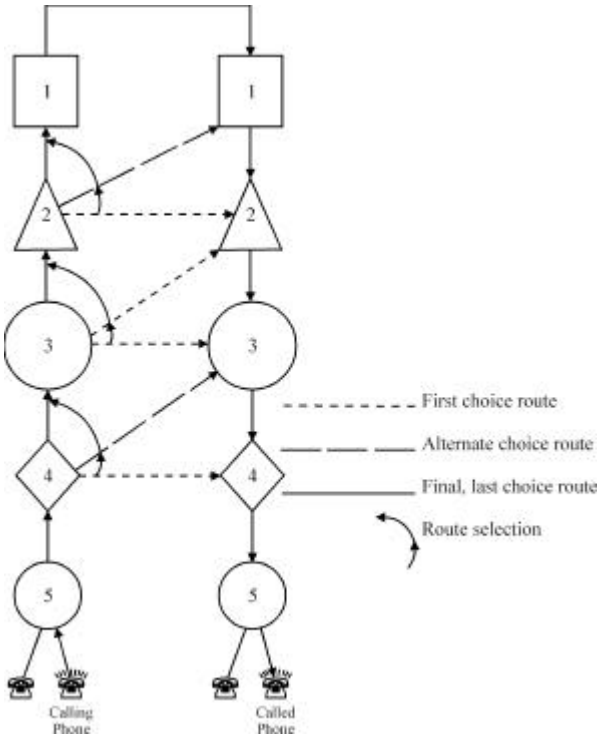

Figure 3. Tiered hierarchy plus high usage trunks.

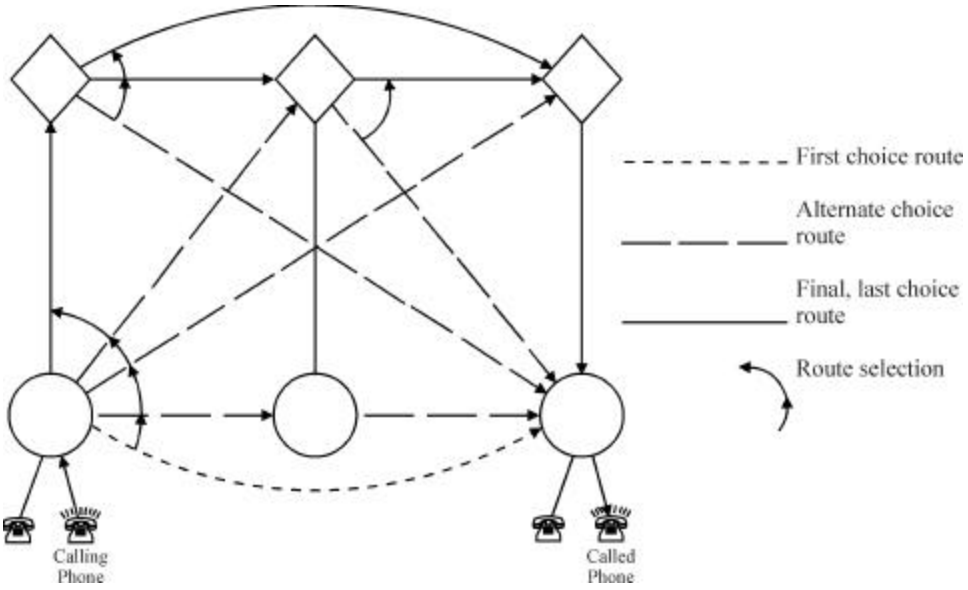

Figure 4. Dynamic nonhierarchical routing.

As with the hierarchical structure, the lowest level is an end office (EO) switch that connects to the end users, as indicated in Figure 5. An EO typically serves 20,000 to 40,000 users with 10,000 to 100,000 users possible, as mentioned above. The loss of an EO would mean that those users connected to that EO would be blacked out (phone line, 911, Internet). The rest of the network would be unaffected, however. The software used in an EO is local. Thus, it is also not expected that a software failure at an EO would propagate further through the system.

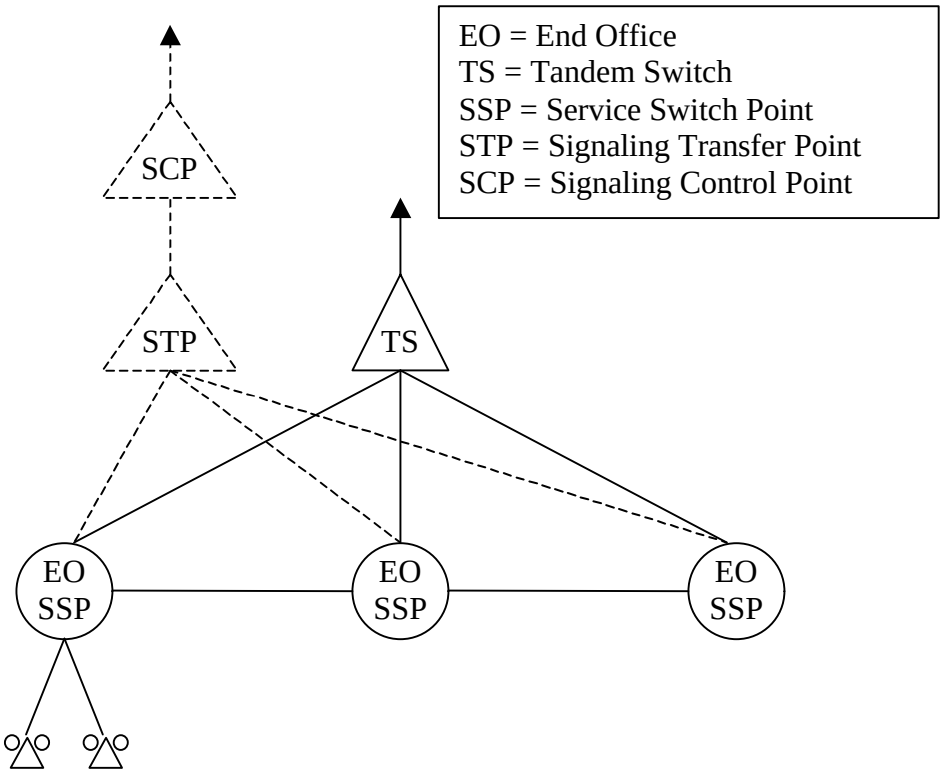

Figure 5. The DNHR switching and signalling hierarchy.

The next level in the DNHR switching network is a tandem switch (TS), which connects local EOs and forms the long distance links (see Fig. 5). The loss of a tandem switch could sever long distance connections (assuming no alternate TS exists); however, it is more likely that another path would be found. With a TS out of service, traffic overflow could cause temporary blackouts. Local connections would remain largely intact due to direct connections between EOs. This could also mean continuation of 911 service.

2.1.1.2 Signaling System

The signaling layer checks for the availability of connections and routes, monitors traffic loads, and controls the system logic (Fig. 5 - dotted lines). At the lowest level is the

service switch point (SSP). If a service switch point (SSP) goes down, local customers could again be affected. One scenario is simply the loss of dial tone. Although EO switching equipment might be intact, the end user will not be able to complete a call if the dial tone is not initiated. If significant numbers of customers load the system trying to obtain a dial tone, the signaling system may experience blocking even in undamaged areas.

The next level is the signaling transfer point (STP). If an STP is disabled, then the status of the end user (line open, line busy) will not be clear and a call may not be completed. The worst scenario is if the final level, a signaling control point (SCP), is out. In this case a call could not be completed. The signaling net has dual redundancy. Dual STPs (and SCPs) are typically physically separated by at least 15 miles. Each dual system is designed to operate at 40% capacity under normal conditions. Thus, if one system goes down, the remaining system is designed to handle the full load at an 80% capacity level. However, the load may exceed capacity if sufficient extra users try to access the system (due to a station loss or a perceived emergency).

Additional potential problems are regionally handled services such as credit card calling, 800 numbers, Internet, and FAA and government circuits. These are usually handled at the SCP level and could be lost if the SCP went down.

In summary, the only portion of the route that does not have alternative connections is from the residence or business to the EO switch. If an EO were to suffer a disaster, the telephones from residences and businesses that are connected to this office's switches would be disabled from the network. However, the loss of an EO (although disastrous to the customers connected to the office directly) does not result in a disaster for the overall PSTN. The worst case would be the loss of one or both STPs (dual redundancy) as these serve a very large number of users. A single STP is designed to have sufficient capacity to handle normal traffic should the other STP be disabled. But abnormal traffic levels or the loss of the second STP could black out the area served (for example a large metro area). It is not expected that the PSTN system would be affected beyond this level.

2.1.2 Internet

The Internet is structured much like the network shown in Figure 4, except that Internet messages are partitioned into a number of smaller packets before transmission. These packets are then reassembled at the destination to form the message. The packets of data do not rely on a "call setup" to construct a single route for the data to flow along from data source to data destination. Instead the packets can all travel different routes from source to destination. With many nodes able to correctly send the data to the proper destination, individual nodes can be removed from the network and the data flow will not be affected except for a loss of redundancy and capacity. The weak link is from the residence or business to the Internet, because as in the PSTN case there is typically no redundancy provided. Thus if the center where the lines to the Internet converge is affected by a disaster, these customers of the Internet will lose their access.

2.1.3 Cellular Mobile Radio Telephone

Cellular mobile telephone service derives its name from the many cells used to partition a large area to be covered. The partitioning of an area into cells allows for channel re-use via frequency, time, or code multiplexing, as well as for lower mobile transmitter power. Present cellular mobile radio systems are summarized in Table 1 [2]. Cellular service provides both PSTN and Internet features to mobile users. The important factor is that the frequencies of operation largely overlap the frequency range (0.8-30 GHz) of the RF devices assumed here.

Table 1. A Comparison of Cellular Mobile Radio Systems

Parameter	AMPS	MCS-L1 MCS-L2	NMT	C450	TACS	GSM	PCN	IS-54
TX Freq., MHz Base Mobile	 869-894 824-849	 870-885 925-940	 935-960 890-915	 461-466 451-456	 935-960 890-915	 890-915 935-960	 1710-1785 1805-1880	 869-894 824-849
Multiple Access	FDMA	FDMA	FDMA	FDMA	FDMA	TDMA	TDMA	TDMA
Duplex Method	FDD	FDD	FDD	FDD	FDD	FDD	FDD	FDD
Channel BW, kHz	30.0	25.0 12.5	12.5	20.0 10.0	25.0	200.0	200.0	30.0
Traffic Channels per RF Channel	1	1	1	1	1	8	16	3
Modulation Type Voice Data	 PM PSK	 PM PSK	 PM PPSK	 PM PSK	 PM PSK	 GMSK GMSK	 GMSK GMSK	 $\pi/4$ $\pi/4$

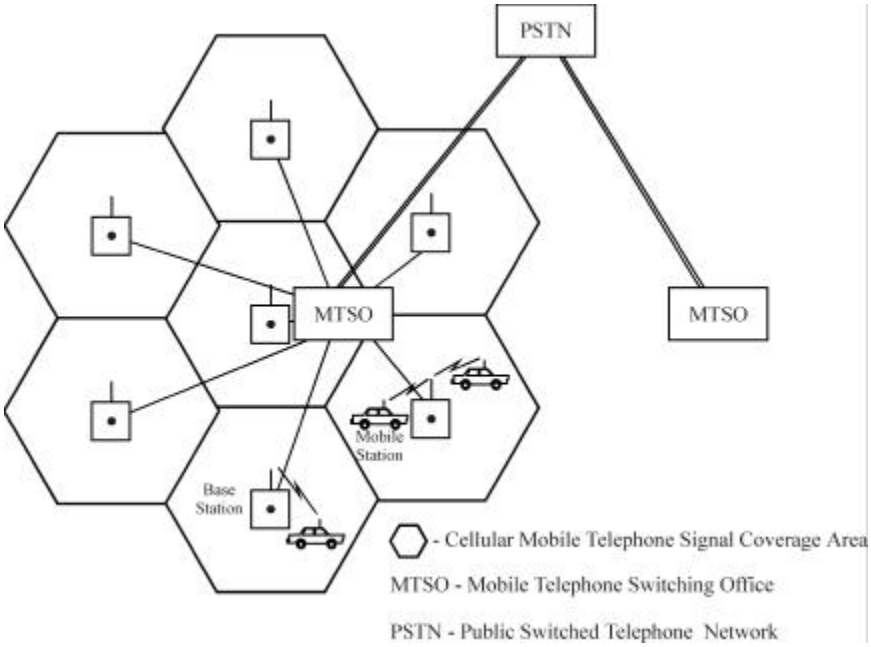

Figure 6. The cellular mobile telephone service network.

Figure 6 shows cells of the system providing wireless signal coverage to mobile users. Control channels at the cell base stations transmit and receive signals from the mobile radios. When the mobile moves beyond the coverage of the serving cell, control channels of adjacent cells measure the received signal strength of the mobile transmitter and determine which cell should take over the call. Although there is some overlap of the signal coverage from adjacent cells, if the base station of a cell were disabled then adjacent cells could not provide complete redundant coverage, nor could they provide sufficient capacity to replace the disabled base station. Figure 6 also shows connections from the base stations of a group of cells to a mobile telephone switching office (MTSO). The number of cells that belong to a particular MTSO depends on the provider, the geographic area being served, and the MTSO manufacturer. Typically, an MTSO serves 50 to 100 cell base stations. If an MTSO were disabled, then the service to all mobile users served by those cells would be terminated. Thus an individual cell's base station or an MTSO would be the vulnerable points in the Cellular Mobile Telephone Service.

The above discussion in regards to the typical operation of a Cellular Mobile Telephone Service also relates to the operation of Personal Communications Service (PCS). PCS systems provide mobile user access to the PSTN and Internet but the cells are much smaller in size. This requires more cell base stations to cover the same geographical area as a cellular service, but the control and functions are similar between the two services.

2.1.4 Private Radio Networks (SMR, Public Safety, Law Enforcement)

Private radio networks are built and administered by the organizations that use them: such as public safety agencies (e.g., fire, police, etc.), land transportation industries (e.g., railroad, trucking, taxi, etc.), industrial services groups (e.g., business, power, petroleum, forest products, etc.), and specialized mobile radio (SMR) providers. The SMR providers build private radio networks for other users and charge a subscription for use. Table 2 summarizes common dispatch systems worldwide [2]. Table 2 is not complete; however, like Table 1, it indicates that many dispatch systems operate within the 0.8 to 30 GHz frequency range considered critical here.

Table 2. A Comparison of Dispatch Systems

Parameter	US	Sweden	Japan	Australia
TX Freq., MHz				
Base	935-940 851-866	76.0-77.5	850-860	865.00-870.00 415.55-418.05
Mobile	824-849 806-821	81.0-82.5	905-915	820.00-825.00 406.10-408.60
Duplex Method	FDD/semi, full	FDD/semi	FDD/semi	FDD/semi, full
Channel BW, kHz	12.5 25.0	25.0	12.5	25.0 12.5
Modulation Type				
Voice	PM	PM	PM	PM
Data	PSK	MSK-PM	MSK-PM	PSK

Private Radio Networks can be local to serve a community, they can cover a county or a state, or they can cover the entire U.S. (e.g., the railroad's radio network). These networks are used for internal communications, control, and administration. They can but usually do not allow the mobile users to gain access to the PSTN or the Internet.

Private radio networks share few common characteristics. There is no typical network design for the systems. The equipment is usually housed in buildings designed to protect the radio components from the elements but not extraordinary electromagnetic signals. The designs do not usually include redundant components, links, or signal coverage. In many cases, disrupting operations at one location could disable a local or county network. An added concern is that some of the national networks run all of their control and dispatch operations from one location.

2.2 Network Level Vulnerability Summary

As discussed above, the public telecommunications networks have built-in redundancy to mitigate transmission failures due to congestion, load, and equipment failures. If the only means of attacking the various networks is through physical or RF devices and not cyber methods, then the networks will suffer from drops in capacity and reliability but not in overall operation. If a single node is disrupted, then the network will continue to operate. The cellular networks have less redundancy in their designs than do the wireline networks. The private radio networks are the most vulnerable, as they are usually designed to provide a service or tool to the owning agency and the network is not the agency's primary business or concern.

Almost all networks have a portion that is connected by a wireline or wireless link to the subscriber or user. These links are not redundant, so that if the link is disrupted or if the EO is disrupted, individual subscribers and users will lose service. Beyond this lowest level that directly connects the user with the network, most networks are robust and designed with high levels of redundancy.

3. NODAL LEVEL VULNERABILITY

The telecommunications networks discussed above all feature nodes where signals are collected or routed. For the PSTN and Internet networks the nodes are the various switching and signaling stations. For the cellular network the nodes are the base stations and MTSO stations. For the private radio and emergency networks the nodes are typically dispatch stations. This section will examine the vulnerability of the various node types to high power RF fields.

3.1 PSTN Switching and Signaling Stations

Switching and signaling stations are located within buildings of sufficient size to house the large amount of equipment involved. The susceptibility of telecommunications systems within buildings or other structures to external RF radiation is a function of the level of RF shielding provided by the building, the layout of the system within the building, and the components comprising the system. The latter two factors are highly complex and beyond the scope of this report. If we assume there exists some estimate of the field level inside a building necessary to cause disruption or damage to a particular system, then the RF shielding of the building can be used as part of a link analysis to determine the distance at which a given source poses a threat. This type of link analysis will not be done here as the RF source and antenna characteristics are not specified. This section seeks to make clear that in such a link analysis the RF shielding contribution of the building is minimal for the frequency range of interest.

In general, electromagnetic energy can penetrate walls constructed of common building materials such as masonry, concrete, wood, and composites. Penetration is possible over a broad range of RF frequencies. RF radiation can also penetrate metal structures at seams, and at apertures such as windows, doors, and ventilation panels. Unless deliberate design and construction efforts are utilized to assure RF shielding over the threat frequency range, it must be assumed that the telecommunication equipment inside of a building is not protected by a particular structure, as discussed in Appendix A.

Strict RF shielding would mean that all or part of the volume housing sensitive equipment would be in a Faraday cage (i.e., a metallic enclosure). It is our understanding from discussions with representatives of telecommunications companies that RF shielding is not generally incorporated into the design of structures used to house telecommunications equipment. Building construction may range from wood in older facilities, to pre-cast concrete, to steel frame structures with non-load bearing walls. In addition to the electrical properties of the construction material, the overall shielding of a particular building will also depend on its geometry (shape, size compared to the incident wavelength) and location (ground parameters, surrounding terrain). Because these factors may vary widely it is difficult to construct a simple, yet general model for building penetration. However, the key component is the shielding effectiveness of building walls.

The shielding properties of a given wall are difficult to generalize because of its finite size, the variability of its material composition, and the variability of the incident RF field. A useful approximation is to idealize the wall as a slab of infinite extent and given thickness, and the incident field as being a plane wave perpendicular to the wall. These idealizations reasonably approximate direct-path RF fields incident on a building and create a worst case scenario where the greatest RF field transmission through the wall occurs.

As an example of the shielding provided by a typical construction type, plane wave penetration of reinforced concrete (a re-bar mesh) is considered in Appendix A. The diameter and spacing of the re-bar is varied to highlight basic trends. The simulations

show that reinforced concrete is a good shield (> 20 dB transmission loss) as long as the re-bar spacing is small compared to a wavelength. Once the re-bar spacing is on the order of a wavelength (or larger) the reinforced concrete provides little intrinsic shielding. For typical re-bar spacing this should occur above a few hundred MHz. Eventually, at very high frequencies (> 30 GHz) the attenuation through the concrete will again provide reasonable shielding (> 20 dB). The conclusion is that buildings made of reinforced concrete do not provide significant shielding from potential RF fields, particularly in the critical 1-5 GHz range. Buildings constructed from other materials will likely show similar results unless intentionally shielded. Thus, nodal sites housed in standard buildings are vulnerable to high power RF fields.

3.2 Cellular Sites

An overview of cellular mobile radio systems is shown in Table 1 [2]. Base station frequencies may be grouped into three bands: 461-466 MHz (C450), 869-960 MHz (AMPS, MCS, NMT, TACS, GSM, IS-54), and 1710-1785 MHz (PCN). The first band is well below the expected frequency range (0.8-30 GHz) for the assumed RF devices. The two higher bands may be subject to in-band excitation, however. The vulnerability of base stations and mobile switching centers is discussed in Sections 3.2.1 and 3.2.2.

3.2.1 Base Stations

A base station consists of an antenna (or an array of antennas), an elevated mount (tower, rooftop, hilltop), an equipment enclosure (box, shed, building), a cable connection between the antenna and equipment enclosure, and either a cable, fiber, or microwave link to the MTSO (see Figure 6). An example of a cellular base station is shown in Figure 7.

The main points of entry are expected to be the antenna, the connecting cable, and the equipment enclosure. Direct antenna or front door coupling will depend on the in-band and out-of-band response of the antenna. Cable coupling is a function of the cable transfer impedance, the field polarization, and the cable location with respect to the mount. Equipment enclosure coupling will depend on the shielding properties of the enclosure, geometry and size, ventilation apertures, access panel gasketing, and any other breaks in the shield integrity.

As most base station antennas are elevated with respect to the surrounding terrain, they will have some form of lightning protection. Typically, lightning protection consists of a low impedance ground path that shunts transient currents away from antennas, cables, and RF equipment. Grounding of exposed components and the use of surge arrestors in cable links are the primary protection measures. The base station grounding system should provide some protection against currents induced by high power RF fields. The key base station elements, antennas, cables, and RF equipment, are considered next.

3.2.1.1 Antennas

Antennas are intentional RF energy transceivers. Cellular base station antenna horizontal plane radiation patterns are either omni-directional (i.e., uniform 360 degree radiation pattern) or sectoral (e.g., covering a 120 degree pie shaped sector). In the vertical plane the beam is narrower and directed along the ground. A typical configuration is three antennas: a single transmit antenna and two receive antennas. The two receive antennas allow for diversity gain, which helps to compensate for the relatively weak mobile transmitter signal.

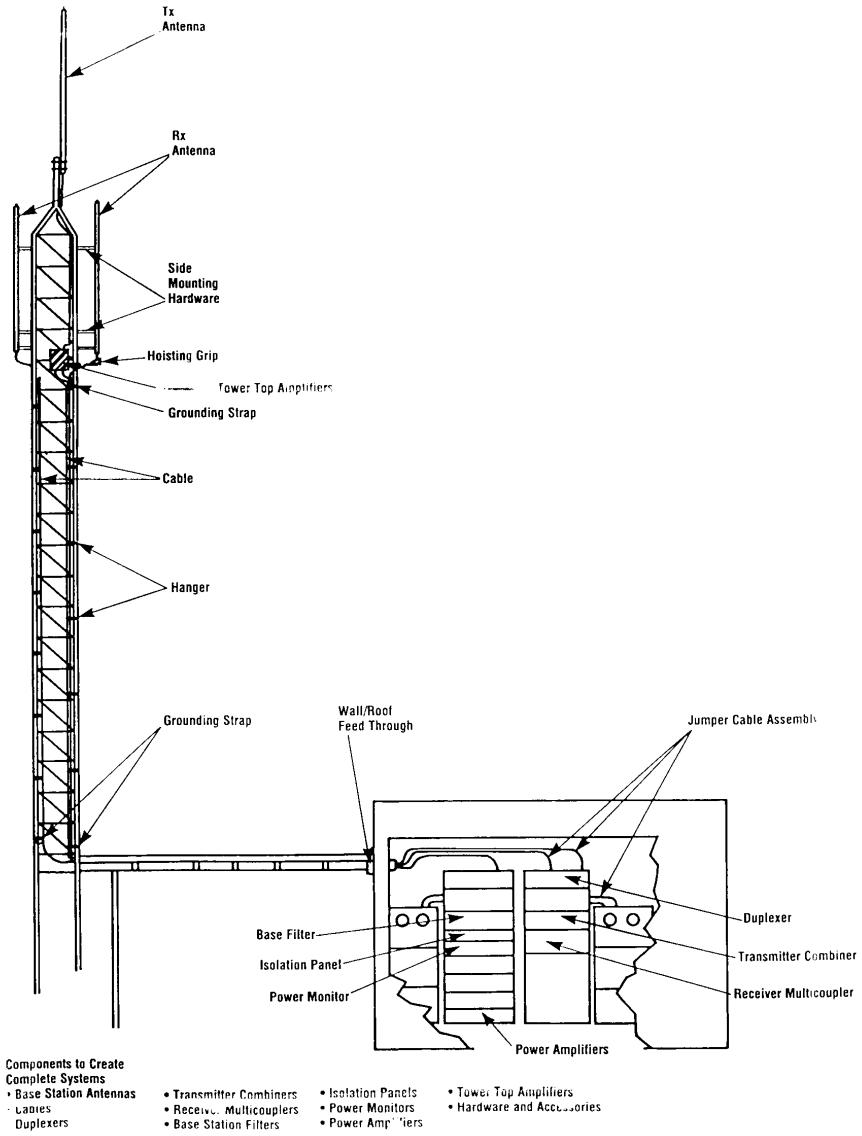

Figure 7. Typical mobile cellular radio telephone base station.

Outdoor antennas consist of metallic elements, linear or planar, often covered with some non-metallic weather protection. The antenna elements themselves are expected to be unaffected by high incident field levels. The antenna usually features a balun (balanced to unbalanced line transformer) or a matching circuit to transition from the antenna impedance (geometry dependent) to its load (typically 50 ohm RF equipment). Proper matching is necessary to achieve maximum power transfer. Most matching circuits are passive devices (pi-networks, transmatch circuits, matching stubs, quarter wave sections, etc.) and should be immune to high levels of RF energy. Thus it is not expected that high power RF fields can directly damage a cellular antenna.

The power received at the antenna p_r may be analyzed using

$$\frac{p_r}{p_t} = \frac{g_r g_t l^2}{(4p\ r)^2} \quad , \tag{1}$$

where p_t is the transmitted power, g_r and g_t are the transmit and receive antenna gains compared to an isotropic antenna, r is the antenna separation in meters, and l is the free space wavelength in meters. In terms of dB (denoted by capital letters) this may be written

$$P_r(dBm) \approx P_t(dBm) + G_r(dBi) + G_t(dBi) - 20\log(f(MHz)) - 20\log(r(m)) + 28\,. \tag{2}$$

These expressions will be of interest in Section 3.2.1.3 where we consider the power delivered by an antenna to an RF amplifier.

3.2.1.2 Cables

Coaxial cables (typically 50 ohm) are used to connect transmit and receive antennas to the RF equipment. Shielded cable is used to provide both interference and weather protection. Both lightning and RF fields can induce currents on the exterior of a coaxial cable. Cellular base stations often feature long runs of cable. The currents induced on the interior of the cable will depend on the basic shielding properties of the cable, cable interruptions (e.g., connections) and possible shield flaws (e.g., cracks or holes). The voltage induced in the interior of a shielded cable due to an external current is detailed in Appendix B.

Two types of shielded cable are considered in Appendix B: rigid (i.e., tubular) and flexible (e.g., braided). Tubular coaxial cable is much like a pipe with a rigid outer conductor. It is often used because it can be pressurized to combat environmental contamination such as moisture. Flexible coaxial cable is more common. The outer and inner conductors are no longer rigid so that the cable can be bent, facilitating routing and connecting. The outer conductor is typically a metallic weave or a spiral wrap.

The analysis in Appendix B shows that, even for long runs of cable, the induced voltages will be insignificant if the shield integrity is intact. A more accurate estimate of cable coupling would involve accounting for the geometry of a specific station, the cable parameters, and the specifics of the incident fields. In addition, any breeches in the cable shield integrity and imperfect connections need to be considered. Based on the transfer quantities for tubular and braided cable, however, it is expected that good quality cable should not allow significant voltages to appear internally.

3.2.1.3 RF Equipment

The RF equipment at a base station can be affected by direct or indirect RF device-generated fields. Direct coupling will be through the front-door antennas used to transmit and receive mobile links. Indirect coupling will be via the antenna-to-RF-equipment connecting cables and via coupling through the enclosure housing the RF equipment. Cable coupling has been briefly discussed above and is not expected to be significant if good quality shielded cable is used. Enclosure coupling is more difficult to assess because of the variety of possible enclosures. However, the standard practice is to use a metal shed or box with metal access panels. Enclosures are not intentionally designed to be RF tight; thus, gasketing is typically non-conductive rubber or equivalent. Non-conductive gasketing performs well as a weather seal but will not ensure a good RF seal. Nonetheless, a metallic enclosure should act as a good shield.

In addition most RF components are themselves housed in metallic cases. Most components will have been tested to FCC (Federal Communications Commission) emission standards (Part 15) and possibly to IEC (International Electrotechnical Commission) immunity standards (61000 series). These ensure that the RF equipment should not act as efficient antennas, either radiating or receiving. Thus, enclosure coupling will pose only a minor threat to the base station RF equipment.

The main threat to base stations is direct in-band coupling (near the frequency of operation) via transmit and receive antennas. The signals received from mobile sources are often very weak. Thus, RF amplifiers are placed close to the antennas within the receiver circuit to boost these weak signals. Normally the amplifiers will be located in a shed along with the other RF equipment. However, as indicated in Figure 7, amplifiers may be mounted up on a tower to help compensate for long cable runs. RF amplifiers can be damaged if overloaded, that is, if the input signal is too large. Under normal conditions this is avoided by limiting the power output of the mobile user. Narrow band RF filters are also placed in the antenna-to-RF equipment link. These filters limit the out-of-band energy received by the antennas from unintended sources. Thus, the main problem is the in-band response of low noise amplifiers. Typical low noise amplifiers have overload thresholds on the order of 10-20 dBm.

As an example, let

$$P_t = 1\ MW = 90\ dBm$$
$$G_r = G_t = 10\ dBi$$
$$f = 1\ GHz = 10^3\ MHz$$
$$r = 1000\ m \quad .$$

Then equation (2) yields

$$P_r(dBm) = 90 + 10 + 10 - 60 - 60 + 28 = 18 \quad .$$

As mentioned, the nominal input damage level for a typical low noise receiver is on the order of 10-20 dBm. Thus, the above example is near the damage threshold. For transmit powers significantly exceeding 1 MW, damage at ranges less than 1 km will be likely. The above example assumes only free space path loss. For areas where vegetation or structures block line of sight, the path losses will be higher. Nonetheless, the elevated location for most base station antennas means that a direct clear path will often be obtainable. Table 3 summarizes the above estimate (equation 2) for 900 MHz and 1800 MHz systems. Transmit (Tx) and receive (Rx) antenna gains of 10 dBi are assumed. A variety of transmit powers and separations are considered. The table clearly shows that overloading base station amplifiers can easily be achieved by high power RF fields. It should also be noted that base stations can be easily jammed even at much lower power levels by transmitting above the power allowed for mobile sources. In summary, base stations are highly vulnerable to RF fields.

Table 3. Base Station Received Power versus Frequency, Transmitter Power, and Transmitter Distance

Frequency (MHz)	900				1800			
Transmit Power (MW)	1	10	100	1000	1	10	100	1000
Tx/Rx Distance (m)	Received Power (dBm)							
100	37	47	57	67	31	41	51	61
300	27	37	47	57	21	31	41	51
500	23	33	43	53	17	27	37	47
1000	17	27	37	47	11	21	31	41
2000	11	22	32	42	5	15	25	35
3000	7	17	27	37	1	11	21	31

3.2.2 Mobile Telephone Switching Offices

MTSOs are similar to the PSTN switching and signaling stations. Thus, the same discussion applies (see Section 3.1), namely, it should be assumed that building construction does not provide shielding from potential RF fields.

3.3 Private Radio Networks Dispatch Stations

Dispatch systems occupy numerous bands in the spectrum. For example, police radio bands exist in the bands 30-50 MHz, 150-174 MHz, 406-470 MHz, and 764-940 MHz [3-5]. Table 2 gives a summary of some dispatch systems worldwide.

The discussion of cellular base station vulnerability (Section 3.2.1.3) also applies to dispatch base stations as these are configured in a very similar manner. Thus, it is expected that the primary threat is the in-band response of the system via direct antenna coupling and the resulting potential to overload RF amplifiers. Assuming that high power RF fields have a nominal 800 MHz lower frequency limit, then most dispatch systems operating below 500 MHz will be safe. Dispatch systems in bands near to 1 GHz will be highly vulnerable, however.

3.4 Nodal Level Vulnerability Summary

Neither PSTN switching stations nor cellular base stations are intentionally hardened against high level RF fields. As a result, both are vulnerable to high-power RF fields. PSTN switching stations are complex installations and the probability of a disruption is hard to predict. Because typical re-bar and concrete construction provides negligible shielding above a few hundred MHz, it can be assumed that fields will penetrate such buildings with the potential to couple to sensitive equipment. Cellular and dispatch base stations are highly vulnerable to high power devices operating in their pass band.

4. CONCLUSIONS

This report has briefly examined the vulnerability of public and private telecommunications systems to be upset and/or damaged by high power RF fields. The basic conclusions reached are:

- Network vulnerability:
    - The overall public telecommunications network has sufficient redundancy and capacity to withstand the loss of even multiple nodes. A full nationwide system collapse is not envisioned as a possible scenario.

- Loss of equipment or the failure of software at a node within the public switched telephone network is not likely to cascade further within the system. Nonetheless, the loss of certain key system nodes could lead to large local blackouts, such as a metro region (greater Denver for example).

- The loss of a base station would largely black out the associated cell. However, adjacent cells should still function.

- The loss of a mobile telephone switching center could black out up to 100 base stations; however, it is not expected that the upset will propagate further within the system.

- Nodal vulnerability:

  - Neither public network switching stations nor cellular base stations are intentionally hardened against high level RF fields.

  - The shielding provided by typical concrete and re-bar construction is negligible for wavelengths on the order of, or smaller than, the re-bar spacing.

  - A switching station could be disrupted, although the probability of disruption is difficult to assess due to the variety and complexity of building layouts. The loss of a switching station would black out the end users connected to that station (typically 10-100 thousand).

  - Wireless base stations are highly vulnerable to high power devices operating within the base station pass band. This conclusion is based on free space link budget calculations. These should be valid approximations for raised base stations. Direct coupling into the system via transmit and receive antennas could easily damage RF amplifiers. The loss of a base station would largely black out the associated cell. However, adjacent cells will still function.

  - Dispatch system base stations are highly vulnerable to high power devices operating within the pass band. To the extent that dispatch systems are stand alone they will not affect other telecommunications systems.

These conclusions are based on a review of telecommunications networks, discussions with providers, and basic estimates of the coupling of RF energy into systems. However, to more accurately assess the threat posed by high power RF fields, more detailed modeling and measurements are needed. In particular, statistics on the transfer function relating a source external to a building and equipment internal to a building need to be developed. This would more accurately define the threat to computer processors and other equipment located within buildings.

5. REFERENCES

[1] M. Wik, R. Gardner and W. Radasky, "Electromagnetic terrorism and adverse effects of high power electromagnetic environments," in *Proc. 13th Intl. Zurich Symp. and Techn. Exhb. on EMC*, Zurich, Switzerland, 1999, pp. 181-185.

[2] J. Gibson, Ed., *The Mobile Communications Handbook*, Boca Raton, FL: CRC Press, 1996, Ch. 15.

[3] G. Leon and L. Sands, *Dial 911: Modern Emergency Communications Networks*, Rochelle Park, NJ: Hayden Book Company, 1975.

[4] Code of Federal Regulations, Title 47-Telecommunication, Part 90, Private Land Mobile Radio Services, Oct. 1996 (Revision).

[5] NTIA, Manual of Regulations and Procedures for Federal Radio Frequency Management, Sept. 1995 (Edition).

[6] K. Yee, "Numerical solution of initial boundary value problems involving Maxwell's equations in isotropic media," *IEEE Transactions on Antennas and Propagation*, AP-14, No. 3, pp. 302-307, May 1966.

[7] A. Taflove, *Computational Electrodynamics: The Finite-Difference Time-Domain Method*, Boston, MA: Artech House, 1995.

[8] K. Lee, Ed., *EMP Interaction: Principles, Techniques, and Reference Data*, Washington, DC: Hemisphere Publishing, 1986, Ch. 2.